Defence Science Journal, Vol. 37, No. 4, October 1987, pp. 423-451

Command, Control, Communication and Intelligence Systems A Review

R.P. Shenoy
Distinguished Scientist
Ex-Director
Electronics and Radar Development Establishment, Bangalore–560 001

ABSTRACT

Command, control, communication and intelligence (C^3I) systems have become a necessity in future battlefield and warfare situations. Even though C^2 to a large extent and C^3I to some extent has been practised since the dawn of civilisation, it is only after the advent of microprocessors in the seventies, that C^3I systems have started to take-off. However, it is basically, a reactive concept and can be made as effective as the user wants it to be.

In this review, it is proposed to deal with three new aspects that will bring in substantial changes in them. These are information availability *vs* combat effectiveness, data fusion and application of artificial intelligence techniques. These aspects are outlined in this paper and their contribution to overall improved performance is brought out at the end.

1. INTRODUCTION

Military operations in future whether limited warfare or strategic exchanges, are likely to be fought under conditions, the like of which have never been experience before. Advances in weapon systems and in electronics have added whole new dimensions to warfare by increasing the range, speed, accuracy and lethality of weapons whereby no area of any country is safe from a direct hit by the potential aggressor. This leads us to a situation where the need to be able to command and control the resources available to successfully fight the aggressor assumes greater importance. To achieve this purpose it is necessary to obtain intelligence that is, to gather information about the enemy, process it in real time for decision making and communicate them through a robust and effective communication network. The concept of integrating the elements of information gathering sensors, information processing computers and the back bone communication network to fulfil the objective of optimising the resources

Received 28 May 1987

has been termed C^3I i.e., Command, Control, Communication and Intelligence. Though C^3I has been practiced as far back as the prehistoric man in his hunt for animal preys physically stronger than him, interest in this as a formal concept emerged in the nineteen seventies largely as a result of the advent of microprocessors.

Unfortunately, due to the wide publicity that has been accorded to C^3I, it has come to be regarded as 'all things to all men' creating considerable confusion in the minds of a large section of people outside of the technical community dealing with these aspects. This confusion is further compounded by the fact that many manufacturers tend to brand virtually every new computer or communication equipment as a C^3I 'force multiplier.' It has to be noted that C^3I is a reactive concept and can accomplish as much or as little as the user requires of it. It primarily calls for the user to state clearly the requirements to be met, in particular a clear enunciation of the different threat scenarios that are likely to be faced. The system designer has to translate these into specifications for the sensors, the data fusion and processing capabilities, the communication network and the software that will enable the system to function as a fully distributed system. The subject of C^3I design is thus very interesting so it is proposed to review the impact of three new techniques/aspects i.e., quantification of information availability in terms of combat effectiveness, data fusion and use of AI techniques which will play very important part in enhancing the effectiveness of future C^3I systems.

2. INFORMATION FRAMEWORK ASPECTS

We can consider a C^3I system as a network of information sources and sinks which can exist together spatially or separated far apart. For example, the command centres can be considered as primarily information centres, i.e., a source-sink pair node, to which intelligence, reconnaissance, logistics, status information, weather etc flows in, while decision regarding deployment, weapon utilisation and additional intelligence needs flow out. These data range from voice in the case of minute to minute direction of tactical operations to authenticated recorded stored messages for large scale computer based information processing and display. These command centres have to be interconnected through switching centres and transmission links that move the information/intelligence from one point to another. It can be easily inferred that without proper sensors and adequate processing capability, these centres can become focii of disinformation, confusion and decision making uncertainty. While it is physically impossible to reduce cuncertainties and delays to zero as this would call for infinite capacity and infinite time respectively, the designer has to work out a compromise between the time delay and degree of uncertainty acceptable so that the response to take action at the right place and in right amount is made possible. Hence one can view the C^3I system in the frame work of information using 'Entropy' as the information measure for assessing effectiveness of information manipulation functions such as surveillance, reconnaissance and intelligence, cover and deception, electronic warfare electronic security etc.

There have been attempts in recent times to quantitatively measure the influence of the amount of knowledge or information possessed by a combatant to combat effectiveness by representing this as an adjustment of the parameters in the differential equations that govern combat outcome. For this purpose one has to express mathematically the entropy or rate of change of entropy of important information-manipulative functions involved in C^3I.

One of the most common information-manipulative functions is active search using a surveillance radar. In this case the exchange of information can be expressed as,

$$p = -ap \qquad (1)$$

where p is the entropy (ignorance of the friendly forces) and a is the positive constant,

$p = dp/dt$ = rate of change in entropy.

The increase in knowledge, that is gained in this case is dependent on the state of knowledge already possessed about a given situation. In other words the more we have to know (or the less we have to know) the more there is to gain (or the less there is to gain) by active search, collection and exchange of information about the situation among the concerned and cooperating combatant groups.

On the other hand in the case of such information manipulative functions as cover and deception (covert collection) the increase gained in our knowledge of the situation is directly proportional to our current knowledge and enemy's current ignorance. The more knowledgeable we are and the more ignorant the enemy is, of the current situation, the more effective we will be in our covert attempts to collect information on enemy's communications, radar emissions, patterns of behaviour etc.

This can be expressed as,

$$p = -b(1-p)q \qquad (2)$$

where q is entropy of enemy of current situation and b is a positive constant.

In the case of electronic warfare, the information manipulation action results in interfering and inhibiting enemy's information collection activities. The purpose is to deceive, confuse and degrade enemy's knowledge of the situation. Therefore in this case, the more we know about the situation the more effective we can be to manipulate and thwart enemy's attempts at information collection. The more the enemy knows about the current situation, the more he has to lose if we are successful in our attempts to deny/deceive him of the knowledge about the situation. We can express this relationship mathematically as,

$$q = c\,(1-p\,)\,(1-q\,) \qquad (3)$$

$q = dq/dt$, where dq/dt is the rate of change of entropy of enemy forces and c a positive constant.

The significance of the evanescence/transitoriness of the information possessed by the combatant is an important factor in future battle situations for both combatants. Hence they have to employ as many means or methods (build in redundancies) to gather information about situation of the other and deny own situation information to the other. Therefore, even when no information manipulation activity such as the ones described above take place, the information state alters. Without an active effort

at collecting information evolving the situation, the state of knowledge will thus degrade. This can be expressed mathematically as,

$$p = d\,(1-p) \qquad (4)$$

where d is a positive constant.

Equations (1) to (4) bring home to us the significance of the sensors as information gathering sources in the design of the C^3I system as these equations model information warfare (information exchange or denial between two combatants) as a time varying process. Neither of the combatants involved in this process can maintain his information advantage indefinitely.

These equations enable us to work out the various operational and design measures to minimise enemy's effectiveness while improving our own capabilities without employing the sensors at cross purposes. For example, the use and scheduling of communication and active surveillance emissions in a staggered fashion in time, space and frequency domains in an unpredictable manner can make the job of the enemy in collecting information difficult as he will not be able to discern a specific pattern out of this. In a similar fashion if we design our communication and surveillance emissions to have low probability intercept with minimum detectable energy over any given frequency band, then these robust systems cannot be easily overcome by enemy countermeasures.

Since the amount of knowledge or information possessed by a combatant influences his combat effectiveness attempts have been made in this direction to evolve a mathematical model. For example, in the case of the ground battle, one can analyse it as made up of two basic elements, namely maneuver and fire. (a) Maneuver is intended to move towards the enemy in order to force him out of his pattern of advance. (b) Fire is intended to support the maneuver by paralysing the enemy even temporarily, until our own forces can gain an advantage and destroy the enemy. If one has perfect knowledge or all the information about the enemy then it is possible to concentrate our fire power more effectively. Thus information can be linked to combat by relating, say, perfect knowledge of one's enemy as equivalent to the effectiveness obtained in aimed fire and complete ignorance as equivalent to the effectiveness obtained in area fire. A beginning has been made in this direction, but more research needs to be carried out with respect to the best means of modelling the coupling of the state of information to combat effectiveness, so that optimum fielding and utilisation of the sensors and the EW systems can be realised.

3. DATA FUSION ASPECTS

The successful utilisation of intelligence/information is dependent on three key factors and that is, sensors, data correlation-fusion and dissemination of the processed information. The sensors used in a C^3I system can be radars, ESM systems, infra-red, low light TV, electro optical systems or even human beings. All of them have diverse ranges upto which information/intelligence can be gleaned, different data rates at which the information can be gathered, various accuracies by which the target

parameters can be obtained, different gradations and probabilities for target detection, recognition and identification, different policies for operation and different spectral coverages as well as different spatial volumes to be searched. If the sensors are colocated then the intelligence processing and fusion leading to target recognition and identification becomes an easy task. In case the sensors are not colocated, then the raw data from the sensors has to be processed at the sensor site up to target detection level and then has to be transmitted to a common processor for correlation and fusion with other reports.

The advantages of information fusion include lower false alarm rates, reduced ambiguities, robust operational performance, extended spatial and temporal coverage, increased confidence, improved detection, enhanced spatial resolution and system reliability and overall improved system performance. Hoever, there are numerous difficulties inherent in this task. Some of these are diminishing signatures of targets, passive operation by the enemy to acquire the data of interest through communication nets, programming of weapon systems to emit for minimum possible time, agility of the threats in several parameters that uniquely characterise the threats etc. All these result in greater difficulties for correlation and tracking and thus create gaps in our understanding of the situation. On our part there is a need to use data from other sources for fusion to improve the tracking and identification of targets. These sources external to the sensors include our military plans and orders of battle, intelligence data on enemy's plans and orders of battle obtained by prisoner interrogation, Comint or other means etc. The architectures of data fusion vary greatly over the wide range of missaion for which C^3I is made use of but there are certain common functions which are embedded in all of them. These are, data association and tracking, data combination and classifications.

3.1 Data association and tracking

Data association is the process which correlates new data or information (targets, reports or tracks) with other bits of information already resident in the data base. Correlation can be among multiple reports in time (sequential sampling) or multiple reports in space (different views from distributed sensors) or both. Any algorithm evolved for data association has to take into consideration the possibility of measurements occuring at different points in time and in space as well as varying accuracies of the sensors and the sensor data being available in differing coordinate systems. The association techniques have been broadly classified into report-to-report, report-to-track and track-to-track categories. In the case of report-to-report technique, a correlation gate or a distance measure is used to accept or reject the hypothesis. If there is a difference in time between the reports then the target motion can be used to adjust the gate criteria and this fact can lead us straight away to discriminate between moving threats and stationary/slow moving targets. Report-to-report motion gives best results when the sensor measuring accuracies are very much high as compared to the target velocities and the target is following a specific trajectory. The sequential time samples of the threat can be utilised to develop the kinematic model so that the correlation performance is enhanced. For report-track and track-to-track association,

all possible pairs of (new data-existing data) assignments are formed with each pair being a tentative assignment. Each of these hypotehsis (pairing) is evaluated by computing the probability or likelihood of this pairing being true, the criteria being a specified distance measure in the correlation space. For multiple sensor data sets or time-sequential data, with each new data there can be a combinatorial explosion unless the data sets are reduced. This can be accomplished by clustering the possible hypotheses into multiple tracks or by pruning those data pairs which do not achieve a preassigned lower values of the score. Many mathematical models have been developed over the years to estimate and predict the kinematic behaviour, the more well known being the alpha-beta filter and the Kalman filter.

3.2 Data combination and classifications

Data combination is the numerical process which uses the multiple sensor measurements to classify the threat into one or more specified categories. Several numerical methods of representing and combining evidence have been evolved over the years and these have been broadly categorised as hard decision or soft decision approaches. In the hard decision approach, it combines declarations of single sensors by such logical rules as majority voting or weighted summation. These hard decision rules work very well when the number of sensors are small in numbers and can be implemented as a loop up table of decisions, one for each possible combination of sensor reports. In the case of soft decisions the quantitative measure of evidence is used for a probabilistic or a possibilistic approach to solve the issue. The classical probabilistic approach uses the Bayesian criterion combining the *a priori* probabilities into a posterior probability for decision making. Possibilistic (fuzzy set) approach attempts represent not only the value of the evidence but also a measure of the ignorance (uncertainty) associated with the measurement. In both these approaches, numerical values representing a degree of belief in the candidate category models or hypotheses are brought out and decision rules are applied to the posterior probabilities to assign threat categories. In practice, soft decision approaches ofer a significant benefit due to integration of all the available information provided by the sensors. They can therefore provide an earlier, longer-range decision because of this.

determine the data necessary to task the sensors. This could include pointing data for electro-optical sensors, tuning data for ESM systems, or statistics for computer driven receivers. The final operation in this sequence takes sensor reports, compares them against the current situation model, updates it on the basis of the new information which could result in a new threat being reported or elimination of an earlier false alarm or disambiguation of an earlier report or a stronger belief in the presence of threat already predicted by the model.

In this case the knowledge base that is needed, will include the models of behaviour of threat systems, their interactions with each other, their capabilities, tactics, doctrine and operating procedures. The behaviour model of the threat systems will depict allowable states, the new states that each state could transition to, the condition for making that transition and any observables associated with the state. The knowledge base should also contain the environmental aspects such as terrain constraints on mobility, sitting, atmospheric effects on sensors, etc. The combination of information in the knowledge based systems occurs in a non-Bayesian manner in that it encodes ignorance explicitly, thereby enabling us to distinguish between ignorance and disbelief. This is very crucial in determining, for example, whether a small likelihood associated with a threat system is due to our having looked at and disregarded it (disbelief) or due to our not having looked but not having any strong reason to believe that it is there (ignorance). The AI approach to inference is superior to the conventional approach in that it can access other sources of data to verify a threat or to eliminate most false alarms or to resolve ambiguities by tasking sensors to acquire specific data that is needed. The AI approach leads to graceful degradation as environmental conditions worsen, due to its inherent ability to supplement poor information from one source with information from other sources.

The role of data fusion in C^3I systems is a critical one and the introduction of multi role sensors as well as the use of AI techniques in threat inferencing holds out a promise of much better system performance as all available data is most effectively used. Data fusion thus provides the human commander with accurate and timely information which has the highest possible degree of certainty.

4. AI AND C^3I SYSTEMS

The likely advantages of using AI techniques in data fusion gives us an opportunity to examine whether this can be employed in other areas of C^3I systems. The large scale use of computers in future C^3I systems will result in increased traffic flow between the different nodes which goes against the requirement that the system should operate with least degradation in the face of intense and extensive Electronic Warfare(EW) in the 1990s. There is thus a need to explore techniques that will bring in significant reductions in the amount of information that must be transferred. The present computer languages and protocols for communications, because of the restrictive use of meanings for symbols and words result in a longer string of characters representing the same information or query than is required with a more natural language. Further,

all the necessary steps including data retrieval and processing need to be explicitly spelt out in the data request. On the other hand if a more natural language were to be used, only the desired information need be requested without requiring to spell out all the intervening steps. Attempts are on hand at a large number of research institutions to develop natural language processors which will accept queries, commands, statements or data in natural language with all the ambiguities associated with them and convert them into necessary steps, data searches, manipulations and inferences in the more formal language of the computer to obtain the desired information. Of course in this case the natural language processor will have to possess the knowledge of the subject matter if it has to resolve correctly the abmiguities in the queries, or data presented to it in natural language. Preliminary studies carried out in USA indicate that there can be a ten to one reduction in the characters required to be exchanged between computers to express an information request. It is possible to abbreviate the normal language queries still further through various standard data compression codes and table look-up techniques. To realise these savings in communication traffic, in a distributed data-base system, multiple language processors front-end each data base so that the natural language queries received from a distant point can be interpreted. It also requires a natural language processor back-ending the user terminal to help determine which data base system to send the data request to. While we would be considerably reducing the data traffic between nodes, the computational burden at each node is substantially enhanced as natural language processing is computationally intensive. The additional computational capability will further help in resolving ambiguities, error and conflicts in the received data at each node by means of previous background knowledge and inferencing mechanisms which are used to check logical consistency in the received data. This ability increases the robustness of the system and enhances the tolerance to communication errors. The added computational burden at the nodes will certainly be worth the savings gained in network bandwidth and enhancement in security.

Another area where AI will improve the performance of C^3I systems is in reducing communication overheads for updating data bases in the distributed data-base configuration. If large knowledge bases are created at each node and if these are oriented around the various objects of interest, then each object oriented frame in the knowledge base can contain sensor measurements, features, parameters, location, information reflecting the rules of behaviour of the object, its default parameters etc. Further, many observed actions of the object, trigger associated events and actions in other targets. These interlinkages are reflected by imbedded procedures which is stored in the information frame associated with that object. It would get activated by the appropriate values and data updates so that past observations are combined with these procedures, default values and rules to infer likely future activities and motions. New observations will not be used for updating unless they tend to modify or contradict the existing knowledge base. Hence updates need only reflect significant changes and not information that can be inferred from the existing knowledge-base. In this case we trade-off communication bandwidth for memory overheads. By additing memory-dependent data such as past observed patterns and object inter dependencies,

the processing overhead for drawing inferences and making predictions based on this data is increased but the frequency of updating is reduced. In an extremely hostile environment where intense EW measures are employed by the enemy, the updates are likely to be noisy and reliable but this would not affect the performance of the system as we have memory dependent data.

5. SUMMARY

The increasing advances in sensor technologies and the steep fall in the prices of processors coupled with better and systematic evolution of software will bring in a number of significant changes in future C^3I systems. The trend to find out ways and means of estimating the quantitative relationship between information availability and combat effectiveness will continue, to obtain an edge over the adversary in overall C^3I system performance by optimum deployment of the sensors and EW systems. The use of multiple sensors will become more common thereby requiring data fusion to lead to target identification. Artificial Intelligence techniques will find increasing use in data fusion, natural language processing to reduce communication traffic and achieve robust performance in the presence of hostile environment.